# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-172648
(43)Date of publication of application : 23.06.2000

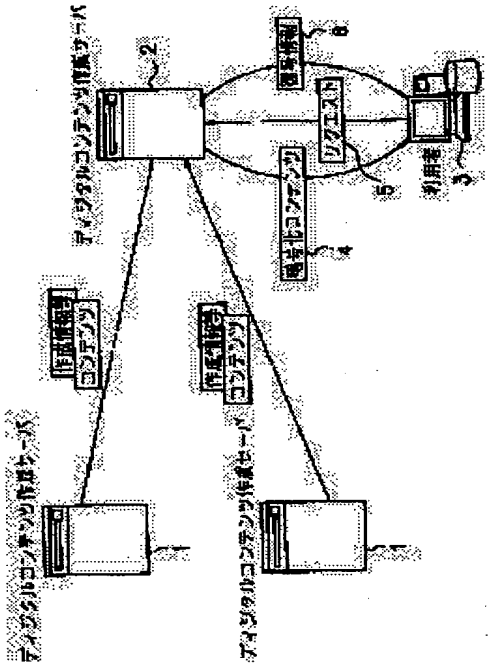
(51)Int.Cl. G06F 15/00
G09C 1/00
G09C 5/00

(21)Application number : 10-351032
(22)Date of filing : 10.12.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : TANAKA KIYOTO
YAMANAKA KIYOSHI
TOMONO AKIRA
KUBOTA YUKIHIRO
HIDAKA TOMOKO
MATSUTANI SHOJI

## (54) DEVICE AND METHOD FOR PROTECTING DIGITAL INFORMATION AND STORAGE MEDIUM WITH DIGITAL INFORMATION PROTECTION PROGRAM RECORDED THEREIN

(57)Abstract:
PROBLEM TO BE SOLVED: To appropriately protect the copyright of digital contents.
SOLUTION: At a distribution server 2, information such as kinds of enciphered digital contents and date of preparation is embedded in these contents by an electronic watermark style so as not to be easily discriminated and not to be easily separated by the third person, and distributed to a user 3 as enciphered contents 4. The user extracts the information, such as the kind of contents and the date of preparation by a program, which is described in an intermediate language form which does not depend on a device, for interpreting and executing the electronic watermark information, applies a digital signature to this information, outputs a request 5 to the distribution server 2 and deciphers the enciphered digital contents while using deciphered information 6 from the distribution server 2 which verifies this request.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－172648
（P2000－172648A）
(43)公開日　平成12年６月23日(2000.6.23)

| (51)Int.Cl.' | 識別記号 | FI | | テーマコード'(参考) |
|---|---|---|---|---|
| G06F 15/00 | 330 | G06F 15/00 | 330Z | 5B085 |
| G09C 1/00 | 620 | G09C 1/00 | 620Z | 5J104 |
| | 640 | | 640Z | 9A001 |
| 5/00 | | 5/00 | | |

審査請求　未請求　請求項の数10　ＯＬ　（全９頁）

(21)出願番号　特願平10－351032

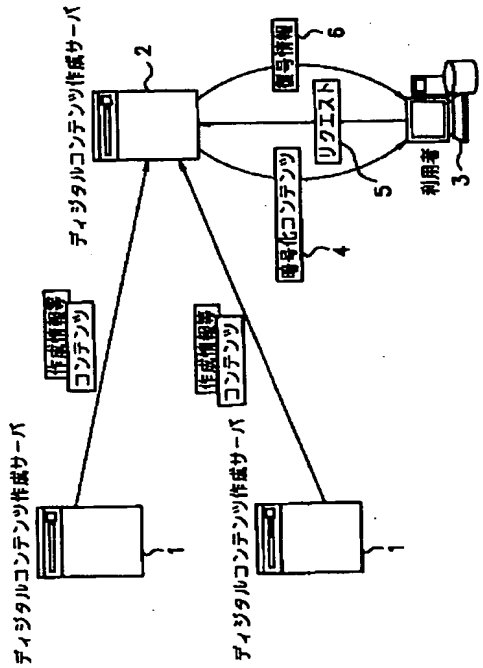
(22)出願日　平成10年12月10日(1998.12.10)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　田中　清人
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内
(72)発明者　山中　喜義
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内
(74)代理人　100069981
弁理士　吉田　精孝

最終頁に続く

(54)【発明の名称】　ディジタル情報保護装置及びディジタル情報保護方法並びにディジタル情報保護プログラムを記録した記憶媒体

(57)【要約】
【課題】　ディジタルコンテンツの著作権を適切に保護し得る装置及びその方法並びにそのプログラムを記録した記憶媒体を提供すること。
【解決手段】　配布サーバ２において、暗号化されたディジタルコンテンツに当該コンテンツの種類、作成日付等の情報を第三者が容易に判別不可能でかつ簡単には分離不可能な電子透かし形式で埋め込み、暗号化コンテンツ４として利用者３に配布し、利用者３は装置に依存しない中間言語形式で記述された、前記電子透かし情報を解釈し実行するためのプログラムにより前記コンテンツの種類、作成日付等の情報を取り出し、これにディジタル署名を施して配布サーバ２にリクエスト５を出し、これを検証した配布サーバ２からの復号情報６を用いて暗号化されたディジタルコンテンツを復号する。



1

【特許請求の範囲】

【請求項１】　画像、音声等のディジタル情報を暗号化して配布するサーバと、該暗号化されたディジタル情報を復号して様々な処理を行う利用者端末とがネットワークを介して接続されてなるシステムにおけるディジタル情報保護装置であって、

サーバは、

暗号化されたディジタル情報の種類等を該暗号化されたディジタル情報に電子透かし情報として埋め込む手段と、

中間言語形式で記述され、前記埋め込まれた電子透かし情報を解釈し実行するための実行プログラムを用意する手段とを備え、

利用者端末は、

サーバから前記実行プログラムをダウンロードする手段と、

ダウンロードした前記実行プログラムにより前記暗号化されたディジタル情報に埋め込まれた電子透かし情報から、前記暗号化されたディジタル情報の種類等を取り出す手段と、

取り出した情報中の前記暗号化されたディジタル情報の種類等と、利用者の名前と、自己署名形式のディジタル証明書とに対して公開鍵暗号方式の秘密鍵でディジタル署名を施し、これらの情報をネットワークを介してサーバに送信する手段とを備え、

また、サーバは、

利用者端末から送信され受信した情報中のディジタル署名を検証し、検証結果が正しければディジタル情報を暗号化するために使用した暗号化鍵を、前記受信した情報中のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で暗号化するとともにディジタル署名を施し、これらの情報をネットワークを介して利用者端末に送信する手段を備えたことを特徴とするディジタル情報保護装置。

【請求項２】　画像、音声等のディジタル情報を暗号化して配布するサーバと、該暗号化されたディジタル情報を復号して様々な処理を行う利用者端末とがネットワークを介して接続されてなるシステムにおけるディジタル情報保護装置であって、

サーバは、

ディジタル情報を共通鍵暗号方式で暗号化するとともに暗号化鍵を保存する手段と、

前記暗号化されたディジタル情報の種類、作成日付、有効期限等をサーバの公開鍵暗号方式の公開鍵で暗号化し、ディジタル署名を施す手段と、

これらの情報及びサーバのディジタル証明書を前記暗号化されたディジタル情報に電子透かし情報として埋め込む手段と、

中間言語形式で記述され、前記埋め込まれた電子透かし情報を解釈し実行するための実行プログラムを用意する

2

手段と、

前記実行プログラムをサーバからダウンロードするためのダウンロードプログラムを前記電子透かし情報が埋め込まれたディジタル情報に付加し、これらの情報を利用者に配布する手段とを備え、

利用者端末は、

前記暗号化されたディジタル情報に付加された前記ダウンロードプログラムを取り出す手段と、

取り出した前記ダウンロードプログラムによりサーバから前記実行プログラムをダウンロードする手段と、

ダウンロードした前記実行プログラムにより公開鍵暗号方式の鍵ペアを生成するとともに、利用者名、当該鍵ペアのうちの公開鍵等を含む自己署名形式のディジタル証明書を作成する手段と、

ダウンロードした前記実行プログラムにより前記暗号化されたディジタル情報に埋め込まれた電子透かし情報から、前記暗号化されたディジタル情報の種類、作成日付、有効期限等、ディジタル署名及びサーバのディジタル証明書を取り出す手段と、

取り出した情報中のディジタル証明書に含まれるサーバの公開鍵暗号方式の公開鍵で、取り出した情報中の前記暗号化されたディジタル情報の種類、作成日付、有効期限等についてのディジタル署名を検証し、検証結果が正しければ前記暗号化されたディジタル情報の種類、作成日付、有効期限等と、利用者の名前と、前記自己署名形式のディジタル証明書とに対して公開鍵暗号方式の秘密鍵でディジタル署名を施し、これらの情報をネットワークを介してサーバに送信する手段とを備え、

また、サーバは、

利用者端末から送信され受信した情報中の自己署名形式のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で、該受信した情報中のディジタル署名を検証する手段と、

検証結果が正しければ受信した情報中のサーバの公開鍵暗号方式の公開鍵で暗号化された部分をサーバの公開鍵暗号方式の秘密鍵で復号する手段と、

復号した情報についてディジタル情報の種類、作成日付、有効期限等を検証し、検証結果が正しければディジタル情報を暗号化するために使用した、保存している共通鍵暗号方式の暗号化鍵を取り出す手段と、

該暗号化鍵を前記受信した情報中の自己署名形式のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で暗号化するとともにディジタル署名を施し、これらの情報をネットワークを介して利用者端末に送信する手段とを備え、

また、利用者端末は、

サーバから送信され受信した情報を、利用者の公開鍵暗号方式の秘密鍵で復号するとともにディジタル署名を検証する手段と、

検証結果が正しければ復号した共通鍵暗号方式の暗号化

鍵を使用して前記暗号化されたディジタル情報を復号する手段とを備えたことを特徴とするディジタル情報保護装置。

【請求項３】　利用者端末におけるディジタル情報の復号結果等のディジタル暗号処理における結果や途中の情報等は、全て利用者端末の揮発性の記憶装置上に格納することを特徴とする請求項１または２記載のディジタル情報保護装置。

【請求項４】　利用者端末で処理が終了あるいは検証結果が正しくない時は直ちに揮発性の記憶装置上の当該データを破棄することを特徴とする請求項３記載のディジタル情報保護装置。

【請求項５】　画像、音声等のディジタル情報を暗号化して配布するサーバと、該暗号化されたディジタル情報を復号して様々な処理を行う利用者端末とがネットワークを介して接続されてなるシステムにおけるディジタル情報保護方法であって、

サーバは、

暗号化されたディジタル情報の種類等を該暗号化されたディジタル情報に電子透かし情報として埋め込み、

中間言語形式で記述され、前記埋め込まれた電子透かし情報を解釈し実行するための実行プログラムを用意し、

利用者端末は、

サーバから前記実行プログラムをダウンロードし、

ダウンロードした前記実行プログラムにより前記暗号化されたディジタル情報に埋め込まれた電子透かし情報から、前記暗号化されたディジタル情報の種類等を取り出し、

取り出した情報中の前記暗号化されたディジタル情報の種類等と、利用者の名前と、自己署名形式のディジタル証明書とに対して公開鍵暗号方式の秘密鍵でディジタル署名を施し、これらの情報をネットワークを介してサーバに送信し、

また、サーバは、

利用者端末から送信され受信した情報中のディジタル署名を検証し、

検証結果が正しければディジタル情報を暗号化するために使用した暗号化鍵を、前記受信した情報中のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で暗号化するとともにディジタル署名を施し、これらの情報をネットワークを介して利用者端末に送信することを特徴とするディジタル情報保護方法。

【請求項６】　画像、音声等のディジタル情報を暗号化して配布するサーバと、該暗号化されたディジタル情報を復号して様々な処理を行う利用者端末とがネットワークを介して接続されてなるシステムにおけるディジタル情報保護方法であって、

サーバは、

ディジタル情報を共通鍵暗号方式で暗号化するとともに暗号化鍵を保存し、



前記暗号化されたディジタル情報の種類、作成日付、有効期限等をサーバの公開鍵暗号方式の公開鍵で暗号化し、ディジタル署名を施し、

これらの情報及びサーバのディジタル証明書を前記暗号化されたディジタル情報に電子透かし情報として埋め込み、

中間言語形式で記述され、前記埋め込まれた電子透かし情報を解釈し実行するための実行プログラムを用意し、

前記実行プログラムをサーバからダウンロードするためのダウンロードプログラムを前記電子透かし情報が埋め込まれたディジタル情報に付加し、これらの情報を利用者に配布し、

利用者端末は、

前記暗号化されたディジタル情報に付加された前記ダウンロードプログラムを取り出し、

取り出した前記ダウンロードプログラムによりサーバから前記実行プログラムをダウンロードし、

ダウンロードした前記実行プログラムにより公開鍵暗号方式の鍵ペアを生成するとともに、利用者名、当該鍵ペアのうちの公開鍵等を含む自己署名形式のディジタル証明書を作成し、

ダウンロードした前記実行プログラムにより前記暗号化されたディジタル情報に埋め込まれた電子透かし情報から、前記暗号化されたディジタル情報の種類、作成日付、有効期限等、ディジタル署名及びサーバのディジタル証明書を取り出し、

取り出した情報中のディジタル証明書に含まれるサーバの公開鍵暗号方式の公開鍵で、取り出した情報中の前記暗号化されたディジタル情報の種類、作成日付、有効期限等についてのディジタル署名を検証し、検証結果が正しければ前記暗号化されたディジタル情報の種類、作成日付、有効期限等と、利用者の名前と、前記自己署名形式のディジタル証明書とに対して公開鍵暗号方式の秘密鍵でディジタル署名を施し、これらの情報をネットワークを介してサーバに送信し、

また、サーバは、

利用者端末から送信され受信した情報中の自己署名形式のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で、該受信した情報中のディジタル署名を検証し、

検証結果が正しければ受信した情報中のサーバの公開鍵暗号方式の公開鍵で暗号化された部分をサーバの公開鍵暗号方式の秘密鍵で復号し、

復号した情報についてディジタル情報の種類、作成日付、有効期限等を検証し、検証結果が正しければディジタル情報を暗号化するために使用した、保存している共通鍵暗号方式の暗号化鍵を取り出し、

該暗号化鍵を前記受信した情報中の自己署名形式のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で暗号化するとともにディジタル署名を施し、これら

の情報をネットワークを介して利用者端末に送信し、
また、利用者端末は、
サーバから送信され受信した情報を、利用者の公開鍵暗号方式の秘密鍵で復号するとともにディジタル署名を検証し、
検証結果が正しければ復号した共通鍵暗号方式の暗号化鍵を使用して前記暗号化されたディジタル情報を復号することを特徴とするディジタル情報保護方法。

【請求項７】　利用者端末におけるディジタル情報の復号結果等のディジタル暗号処理における結果や途中の情報等は、全て利用者端末の揮発性の記憶装置上に格納することを特徴とする請求項５または６記載のディジタル情報保護方法。

【請求項８】　利用者端末で処理が終了あるいは検証結果が正しくない時は直ちに揮発性の記憶装置上の当該データを破棄することを特徴とする請求項７記載のディジタル情報保護方法。

【請求項９】　画像、音声等のディジタル情報を暗号化して配布するサーバと、該暗号化されたディジタル情報を復号して様々な処理を行う利用者端末とがネットワークを介して接続されてなるシステムにおけるディジタル情報保護プログラムを記録した記憶媒体であって、
前記プログラムは、
サーバを構成するコンピュータに、
暗号化されたディジタル情報の種類等を該暗号化されたディジタル情報に電子透かし情報として埋め込み、
中間言語形式で記述され、前記埋め込まれた電子透かし情報を解釈し実行するための実行プログラムを用意する動作を実行させ、
利用者端末を構成するコンピュータに、
サーバから前記実行プログラムをダウンロードし、
ダウンロードした前記実行プログラムにより前記暗号化されたディジタル情報に埋め込まれた電子透かし情報から、前記暗号化されたディジタル情報の種類等を取り出し、
取り出した情報中の前記暗号化されたディジタル情報の種類等と、利用者の名前と、自己署名形式のディジタル証明書とに対して公開鍵暗号方式の秘密鍵でディジタル署名を施し、これらの情報をネットワークを介してサーバに送信する動作を実行させ、
また、サーバを構成するコンピュータに、
利用者端末から送信され受信した情報中のディジタル署名を検証し、
検証結果が正しければディジタル情報を暗号化するために使用した暗号化鍵を、前記受信した情報中のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で暗号化するとともにディジタル署名を施し、これらの情報をネットワークを介して利用者端末に送信する動作を実行させることを特徴とするディジタル情報保護プログラムを記録した記憶媒体。



【請求項１０】　画像、音声等のディジタル情報を暗号化して配布するサーバと、該暗号化されたディジタル情報を復号して様々な処理を行う利用者端末とがネットワークを介して接続されてなるシステムにおけるディジタル情報保護プログラムを記録した記憶媒体であって、
前記プログラムは、
サーバを構成するコンピュータに、
ディジタル情報を共通鍵暗号方式で暗号化するとともに暗号化鍵を保存し、
前記暗号化されたディジタル情報の種類、作成日付、有効期限等をサーバの公開鍵暗号方式の公開鍵で暗号化し、ディジタル署名を施し、
これらの情報及びサーバのディジタル証明書を前記暗号化されたディジタル情報に電子透かし情報として埋め込み、
中間言語形式で記述され、前記埋め込まれた電子透かし情報を解釈し実行するための実行プログラムを用意し、
前記実行プログラムをサーバからダウンロードするためのダウンロードプログラムを前記電子透かし情報が埋め込まれたディジタル情報に付加し、これらの情報を利用者に配布する動作を実行させ、
利用者端末を構成するコンピュータに、
前記暗号化されたディジタル情報に付加された前記ダウンロードプログラムを取り出し、
取り出した前記ダウンロードプログラムによりサーバから前記実行プログラムをダウンロードし、
ダウンロードした前記実行プログラムにより公開鍵暗号方式の鍵ペアを生成するとともに、利用者名、当該鍵ペアのうちの公開鍵等を含む自己署名形式のディジタル証明書を作成し、
ダウンロードした前記実行プログラムにより前記暗号化されたディジタル情報に埋め込まれた電子透かし情報から、前記暗号化されたディジタル情報の種類、作成日付、有効期限等、ディジタル署名及びサーバのディジタル証明書を取り出し、
取り出した情報中のディジタル証明書に含まれるサーバの公開鍵暗号方式の公開鍵で、取り出した情報中の前記暗号化されたディジタル情報の種類、作成日付、有効期限等についてのディジタル署名を検証し、検証結果が正しければ前記暗号化されたディジタル情報の種類、作成日付、有効期限等と、利用者の名前と、前記自己署名形式のディジタル証明書とに対して公開鍵暗号方式の秘密鍵でディジタル署名を施し、これらの情報をネットワークを介してサーバに送信する動作を実行させ、
また、サーバを構成するコンピュータに、
利用者端末から送信され受信した情報中の自己署名形式のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で、該受信した情報中のディジタル署名を検証し、
検証結果が正しければ受信した情報中のサーバの公開鍵

暗号方式の公開鍵で暗号化された部分をサーバの公開鍵暗号方式の秘密鍵で復号し、
復号した情報についてディジタル情報の種類、作成日付、有効期限等を検証し、検証結果が正しければディジタル情報を暗号化するために使用した、保存している共通鍵暗号方式の暗号化鍵を取り出し、該暗号化鍵を前記受信した情報中の自己署名形式のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で暗号化するとともにディジタル署名を施し、これらの情報をネットワークを介して利用者端末に送信する動作を実行させ、
また、利用者端末を構成するコンピュータに、
サーバから送信され受信した情報を、利用者の公開鍵暗号方式の秘密鍵で復号するとともにディジタル署名を検証し、
検証結果が正しければ復号した共通鍵暗号方式の暗号化鍵を使用して前記暗号化されたディジタル情報を復号する動作を実行させることを特徴とするディジタル情報保護プログラムを記録した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像、音声等のディジタル情報（ディジタルコンテンツ）をネットワークやＣＤ－ＲＯＭを介して配布する際の著作権を保護するための装置及びその方法並びにそのプログラムを記録した記憶媒体に関するものである。

【０００２】

【従来の技術】近年、ディジタルコンテンツの流通に適したインターネットの爆発的な普及や、ディジタルコンテンツに対し表示、再生等の様々な処理を行うことのできるパーソナルコンピュータ等の高機能、高性能化に伴い、ネットワークやＣＤ－ＲＯＭを介して配付されたディジタルコンテンツの利用が盛んになっている。

【０００３】ところで、ディジタルコンテンツの場合、ディジタル信号の特性上、コピーを何世代に亘って行っても品質が劣化しないため、正規のユーザ（利用者）以外の者が複製品を利用する、いわゆる違法コピー等の著作権の侵害行為が行われ易い。

【０００４】そこで、コンテンツの著作権を厳しく保護しようとする場合、コンテンツをディジタル暗号技術により暗号化して配付し、正規の利用者には暗号化されたコンテンツを復号する暗号鍵を配付することによりその利用を可能とする等の方法が採られていた。

【０００５】

【発明が解決しようとする課題】しかし、上述のように暗号化したコンテンツを配付し、正規の利用者に暗号鍵を配付する場合、一般に、使用期限や正規の利用者かどうかを判別する情報については暗号化したコンテンツとは別の領域、即ちコンテンツのヘッダ情報等に格納していたため、容易にヘッダ領域から利用者や当該コンテンツに関する情報等を除去したり、別のデータに書き替えて不正な行為を行うことができるという欠点があった。また、以前に配付された暗号鍵を使用して、使用期限が終了した後も当該コンテンツを使用できるという欠点があった。

【０００６】本発明の目的は、ディジタルコンテンツの著作権を適切に保護し得る装置及びその方法並びにそのプログラムを記録した記憶媒体を提供することにある。

【０００７】

【課題を解決するための手段】本発明では上記目的を達成するため、暗号化されたディジタル情報に第三者が容易に判別不可能で、かつ簡単には分離不可能な電子透かし（例えば、中村高雄、小川宏、高嶋洋一「ディジタル画像の著作権保護のための周波数領域における電子透かし方式」（１９９７年　暗号と情報セキュリティシンポジウム（ＳＣＩＳ９７）２６Ａ）、井上彰「電子透かし」（丸山学芸図書）、「『電子透かし』がマルチメディア時代を守る」（日経エレクトロニクス、１９９７、２－２４（Ｎｏ．６８３）、ｐｐ．９９－１２４）参照）形式で当該ディジタル情報の種類、作成日付等の情報を挿入し、これらの形式で利用者にディジタル情報を配付する。さらに、埋め込まれた電子透かし情報を解釈し実行するための中間言語形式のプログラムを用意する。

【０００８】また、本発明では上記目的を達成するため、画像、音声等のディジタル情報を暗号化して配布するサーバと、該暗号化されたディジタル情報を復号して様々な処理を行う利用者端末とがネットワークを介して接続されてなるシステムにおいて、ディジタル情報を配付するサーバは、利用者に配付するディジタル情報を共通鍵暗号方式で暗号化するとともに暗号化鍵を保存する。

【０００９】サーバはディジタル情報の種類、作成日付、有効期限等をサーバの公開鍵暗号方式の秘密鍵で暗号化し、さらに当該情報についてディジタル署名を施し、これらの情報及びサーバのディジタル証明書を前記暗号化されたディジタル情報に第三者が容易に判別不可能な電子透かし情報の形式で挿入する。

【００１０】次に、装置に依存しない中間言語形式で記述され、挿入された電子透かし情報を解釈し実行するためのプログラムを用意するとともに、当該プログラムをサーバからダウンロードするためのダウンロードプログラムを、電子透かし情報が埋め込まれたディジタル情報に付け加えることにより、利用者に配布するディジタル情報を作成する。

【００１１】ディジタル情報を利用者に配付する時は、前記サーバにより作成されたディジタル情報とし、利用者が暗号化されたディジタル情報を使用する時は、配付されたディジタル情報に付け加えられたダウンロードプログラムを使用してサーバからプログラムをダウンロー

ドする。

【００１２】利用者はこのダウンロードしたプログラムを実行することにより公開鍵暗号方式の鍵ペアを生成するとともに、利用者名、当該鍵ペアのうちの公開鍵等を含む自己署名形式のディジタル証明書を作成する。さらにダウンロードしたプログラムを実行することにより暗号化されたディジタル情報に挿入された電子透かし情報を取り出し、取り出した情報中のサーバのディジタル証明書について公開鍵暗号方式の公開鍵を取り出し、さらに電子透かし情報から取り出した暗号化されたディジタル情報の種類、作成日付、有効期限等についてディジタル署名を検証する。

【００１３】次に、暗号化されたディジタル情報の種類、作成日付、有効期限等と、利用者の名前と、利用者の自己署名形式のディジタル証明書と、これらの情報に対する利用者のディジタル署名をサーバに送信する。

【００１４】サーバは利用者からの情報を受信したなら、利用者の自己署名形式のディジタル証明書から取り出した公開鍵で受信情報が正しいか検証する。検証結果が正しければサーバは受信情報に含まれる暗号化された情報を保存しているサーバの公開鍵暗号の秘密鍵で復号し、受信した情報についてディジタル情報の種類、作成日付、有効期限等を検証する。

【００１５】これらの検証結果も正しければディジタル情報を暗号化するために使用した保存されている暗号化鍵を取り出し、該暗号化鍵を前記受信情報に含まれた利用者の自己署名形式のディジタル証明書から取り出した利用者の公開鍵で暗号化するとともにディジタル署名を生成する。暗号化した暗号化鍵情報とディジタル署名を利用者へ送信する。

【００１６】利用者は送信情報を受信したなら、ダウンロードしたプログラムを使用して自己署名形式のディジタル証明書に対応する秘密鍵で暗号化された暗号化鍵を復号するとともにディジタル署名を検証する。検証結果が正しければ復号した暗号化鍵で暗号化されたディジタル情報を復号し、当該情報を表示、印刷等の処理を行う。

【００１７】また、利用者端末におけるディジタル情報の復号結果等のディジタル暗号処理における結果や途中の情報等は、全て利用者端末の揮発性の記憶装置上に格納する。さらに、利用者端末で処理が終了あるいは検証結果が正しくない時は直ちに揮発性の記憶装置上の当該データを破棄することにより、ディジタルコンテンツの不正な利用を防ぐ。

【００１８】本発明によれば、ネットワーク上でディジタル情報を配付し、使用者が表示、再生等の処理を行う場合、これらのディジタル情報の著作権について最適な保護手段を提供できる。

【００１９】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について説明する。

【００２０】図１は、本発明によるディジタル情報保護システムの実施の形態の一例を示すもので、図中、１はディジタルコンテンツを作成するサーバ、２はサーバ１で作成されたディジタルコンテンツを利用者に配付するサーバ、３は利用者が使用する端末装置（利用者端末）であり、これらは図示しないネットワークで接続されている。

【００２１】本システムの概略を、図１を使用して説明する。

【００２２】ディジタルコンテンツは作成者がディジタルコンテンツ作成サーバ１で作成し、作成したディジタルコンテンツと該コンテンツに関する作成情報等をディジタルコンテンツ配付サーバ２に送信する。ディジタルコンテンツ配付サーバ２は受信したディジタルコンテンツについて、利用者に配付するためのディジタル情報を作成し、これらを暗号化コンテンツ４として利用者３に配付する。利用者への配付はネットワークで行ったり、ＣＤ－ＲＯＭのような媒体の形式で配付しても良い。

【００２３】利用者３は配付された暗号化コンテンツ４を利用する時は、配付サーバ２に所定の情報をリクエスト（利用要求）５として送信する、配布サーバ２はリクエスト５を受信したならその内容を検査し、正しければディジタルコンテンツを暗号化するために使用した暗号化鍵を復号情報６として利用者３に送信する。利用者３は復号情報６を使用して元のディジタルコンテンツに戻し、表示や印刷の処理を行う。

【００２４】これらの処理について、図２乃至図４を使用して詳細に説明する。

【００２５】図２は図１中の暗号化コンテンツ４の形式を示しており、図３はディジタルコンテンツ配布サーバ２で配付するディジタルコンテンツを作成する時の処理を示すフローチャート、図４は配付されたディジタルコンテンツを使用する時の処理を示すフローチャートである。

【００２６】ディジタルコンテンツ配布サーバ２で図２の情報を作成する時は、まず、ディジタルコンテンツを暗号化するための共通鍵暗号方式の暗号化鍵を生成し、本暗号化鍵を使用してディジタル情報を暗号化する（ｓ１１）。次に、本ディジタルコンテンツに関する情報、即ち種類、作成日付、有効期限、識別番号、作成者、ディジタルコンテンツ配布サーバ２のアドレス等を、ディジタルコンテンツ配布サーバ２の公開鍵暗号方式の公開鍵で暗号化する（ｓ１２）。ｓ１２で作成した情報にディジタル署名を施し（ｓ１３）、配付途中での情報の改ざんを防ぐ。

【００２７】次に、ｓ１２で暗号化したディジタルコンテンツに関する情報、ｓ１３で作成したディジタル署名及び配布サーバ２のディジタル証明書をｓ１１で作成した暗号化ディジタルコンテンツに、第三者が検知できな

いような電子透かし形式で埋め込む（ｓ１４）。

【００２８】また、一方、電子透かし情報として埋め込んだ情報を取り出し、解釈し実行する実行プログラムを、機種に依存しない中間言語形式で用意する（ｓ１５）。

【００２９】さらに、ｓ１５のプログラムをダウンロードするための中間言語形式の通信用（ダウンロード）プログラムを作成し、ｓ１４の情報に付け加える（ｓ１６）。ｓ１６で作成した情報を利用者に配付する（ｓ１７）。配付手段としては、ネットワークを使用して電子的に行っても、ＣＤ－ＲＯＭのような形態で配付しても良く、その配付形態は問わない。

【００３０】さて、配付されたディジタル情報を利用者が使用する方法について、図４のフローチャートを用いて説明する。ここで、ｓ２１～ｓ２８は利用者端末３の処理であり、ｓ３１～ｓ３４は配付サーバ２の処理である。

【００３１】利用者は配付されたディジタル情報から図２に示すダウンロードを行うための通信用中間言語プログラムを取り出す（ｓ２１）。本プログラムはただ単に付加された形式であるので、利用者は容易に取り出すことができる。また、機種に依存しない中間言語形式、例えばＪＡＶＡアプレットのようなものであるので、ＪＡＶＡのような中間言語プログラムを実行する機能を有していれば、どのような機種でも実行可能である。

【００３２】さて、ｓ２１で取り出したダウンロードプログラムにより、図３のｓ１５で用意した実行プログラムを配付サーバ２によりダウンロードする（ｓ２２）。次に、ｓ２２でダウンロードした実行プログラムを使用して、公開鍵暗号方式における利用者用の公開鍵と秘密鍵の鍵ペアを生成するとともに、自分の秘密鍵で署名した自己署名形式のディジタル証明書を作成する（ｓ２３）。

【００３３】次に、配付されたディジタル情報に電子透かしの形態で埋め込まれた情報を、ｓ２２でダウンロードしたプログラムにより取り出す（ｓ２４）。

【００３４】取り出した情報中のディジタル証明書に含まれる配付サーバ２の公開鍵暗号方式の公開鍵により、取り出した情報中の前記暗号化されたディジタルコンテンツの種類、作成日付、有効期限等についてのディジタル署名を検証する。検証結果が正しければ、ｓ２４で取り出した、暗号化されたディジタルコンテンツの種類、作成日付、有効期限等の情報と、利用者の名前と、ｓ２３で作成した自己署名形式のディジタル証明書とに対して利用者の公開鍵暗号方式の秘密鍵でディジタル署名を行う（ｓ２５）。

【００３５】次に、ｓ２４で取り出した、暗号化されたディジタルコンテンツの種類、作成日付、有効期限等の情報と、利用者名と、ｓ２３で作成した自己署名形式のディジタル証明書と、ディジタル署名した結果をネットワークを介して配付サーバ２へ送信する（ｓ２６）。

【００３６】配付サーバ２はｓ２６で送信され受信した情報中の自己署名形式のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵で、該受信した情報中のディジタル署名を検証する（ｓ３１）。ディジタル署名の検証結果が正しければ、利用者から送信された情報のうち、図３のｓ１２の処理で作成された暗号化情報を取り出し、それを配布サーバ２の公開鍵暗号方式の秘密鍵で復号する（ｓ３２）。

【００３７】復号した情報についてディジタルコンテンツの種類、作成日付、有効期限等を検証し、それが正しければ、図３のｓ１１でディジタルコンテンツそのものを暗号化するのに使用した暗号化鍵を保存してあるところから取り出し（ｓ３３）、次に、この暗号化鍵を受信した情報中の利用者の自己署名形式のディジタル証明書に含まれる利用者の公開鍵暗号方式の公開鍵により暗号化し、さらにディジタル署名を施し、これらの情報をネットワークを介して利用者３へ送信する（ｓ３４）。

【００３８】利用者３はｓ３４の処理で配付サーバ２から送信された情報を受信したなら、その情報を利用者の公開鍵暗号方式の秘密鍵で復号するとともに、ディジタル署名を検証する（ｓ２７）。ディジタル署名の検証結果が正しければｓ１１で暗号化されたディジタルコンテンツを復号した暗号化鍵を使用して復号し、その結果を画面に表示したり、印刷したりする（ｓ２８）。

【００３９】利用者端末３におけるこれらの処理は全て揮発性のメモリ上で実行・格納され、不揮発性の記憶装置上では行わない。また、検証結果が不正な時や、途中で処理を中断する時は、利用者端末３で実行している状態や情報は直ちに破棄する。

【００４０】

【発明の効果】以上説明したように、本発明によれば、ネットワーク上でディジタル情報を配付し、使用者が表示、再生等の処理を行う場合、これらのディジタル情報について有効期限等のチェックができ、不正な利用を防ぐことができる。

【図面の簡単な説明】

【図１】本発明の実施の形態の一例を示すシステム構成図

【図２】利用者に配付する暗号化されたディジタルコンテンツの形式を示す説明図

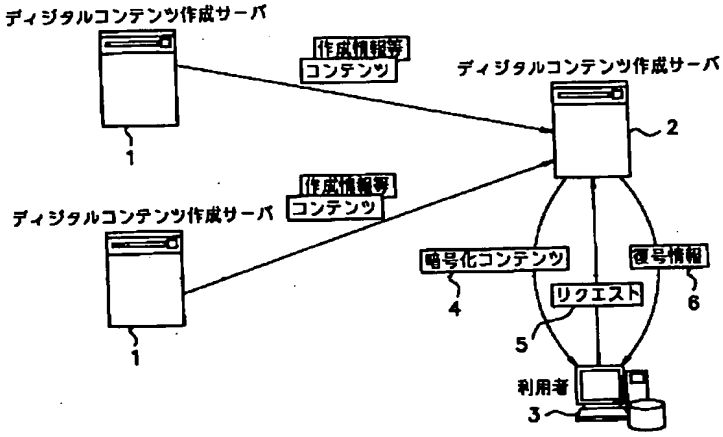
【図３】配付するディジタルコンテンツの作成時の処理フローチャート

【図４】配付されたディジタルコンテンツの使用時の処理フローチャート

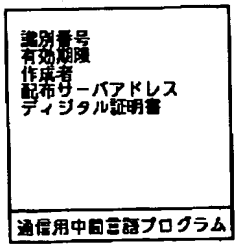
【符号の説明】

１：ディジタルコンテンツ作成サーバ、２：ディジタルコンテンツ配付サーバ、３：利用者、４：暗号化コンテンツ、５：リクエスト、６：復号情報。

【図１】

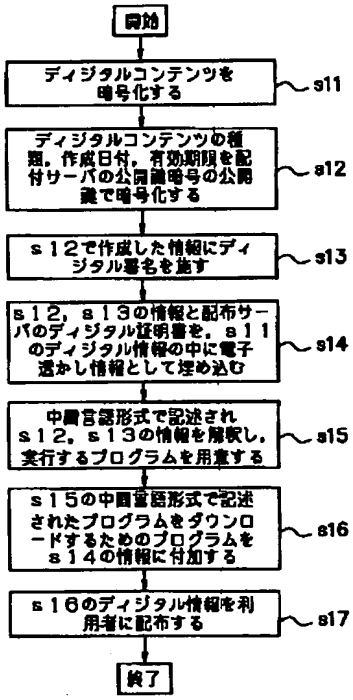



【図２】



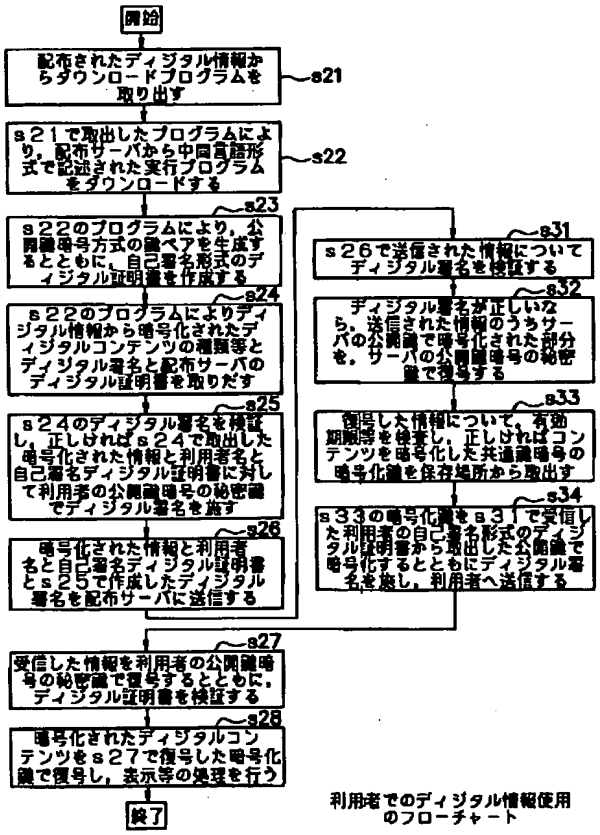

配布ディジタル情報の形式

【図３】




利用者へ配布するディジタル情報の作成フローチャート

【図４】




利用者でのディジタル情報使用のフローチャート

フロントページの続き

(72)発明者　伴野　明
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内
(72)発明者　久保田　幸宏
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内
(72)発明者　日高　朋子
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内
(72)発明者　松谷　章司
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5B085 AE06 AE13 AE29
5J104 AA01 AA09 AA14 EA19 KA01 KA05 NA02 NA37 PA07 PA14
9A001 BB02 BB03 BB04 CC03 DD10 DZ02 EE03 JJ13 JJ18 JJ25 JJ27 KK60 KZ11 LL03

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

---

## CLAIMS

---

[Claim(s)]
[Claim 1] The server which enciphers and distributes digital information, such as an image and voice, and the user terminal which decodes the this enciphered digital information and performs various processings are the digital information protective devices in the system which it comes to connect through a network. A server The means which embeds the class of enciphered digital information etc. as digital-watermarking information at the this enciphered digital information, It is described in an intermediate-language format and has a means to prepare the executive program for interpreting and performing said embedded digital-watermarking information. A user terminal From a means to download said executive program from a server, and the digital-watermarking information embedded by said downloaded executive program at said enciphered digital information The class of the means which takes out the class of said enciphered digital information etc., and said enciphered digital information in the taken-out information etc., A digital signature is given with the private key of a public key cryptosystem to a user's identifier and the digital certificate of a self-signature format. It has a means to transmit such information to a server through a network. Moreover, a server The digital signature in the information which it was transmitted from the user terminal and received is verified. The encryption key used in order to encipher digital information, if a verification result is right The digital information protective device characterized by having a means to give a digital signature while enciphering with the public key of a user's public key cryptosystem contained in the digital certificate in said received information, and to transmit such information to a user terminal through a network.
[Claim 2] The server which enciphers and distributes digital information, such as an image and voice, and the user terminal which decodes the this enciphered digital information and performs various processings are the digital information protective devices in the system which it comes to connect through a network. A server A means to save an encryption key while enciphering digital information with a common key encryption system,

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the storage which recorded the program on the equipment and its approach list for protecting the copyright at the time of distributing digital information (digital contents), such as an image and voice, through a network or CD-ROM.
[0002]
[Description of the Prior Art] In recent years, use of the digital contents distributed through the network or CD-ROM prospers with high efficiency, such as the explosive spread of the Internet suitable for circulation of digital contents, and a personal computer which can perform various processings of a display, playback, etc. to digital contents, and high-performance-izing.
[0003] By the way, since in the case of digital contents quality does not deteriorate even if it covers what generation and performs a copy on the property of a digital signal, the infringement action of copyrights, such as the so-called illegal copy, that persons other than the user (user) of normal use a replica is easy to be performed.
[0004] Then, when it was going to protect the copyright of contents severely, approaches, such as enabling the use, were taken by enciphering with a digital code technique, distributing contents, and distributing the cryptographic key which decodes the enciphered contents among the user of normal.
[0005]
[Problem(s) to be Solved by the Invention] However, since it stored in the header information of a field different from the contents generally enciphered about the information which distinguishes whether you are the user of the expiration date or normal, i.e., contents, etc. when the contents enciphered as mentioned above were distributed and a cryptographic key was distributed among the user of normal, there was a fault that a user, the information about the contents concerned, etc. are easily removable from a header field, or it could rewrite to another data and an unjust action could be performed. Moreover, the cryptographic key distributed before was used, and even after the expiration date was completed, there was a fault that the contents concerned could be used.
[0006] The purpose of this invention is to offer the storage which recorded the program on the equipment which can protect the copyright of digital contents appropriately, and its approach list.
[0007]
[Means for Solving the Problem] Since the above-mentioned purpose is attained in this invention, a third person cannot distinguish easily to the enciphered digital information. and — easy — non-detachable digital watermarking (it Ogawa-** for example, Takao Nakamura —) The digital-watermarking method in the frequency domain for the protection of copyrights of a Yoichi Takashima "digital image" (1997 codes and information security symposium (SCIS97) 26A), Inoue ** "digital-watermarking" (Maruyama Gakugei Tosho) ""digital-watermarking" keeps multimedia age" (the Nikkei electronics —) Information, such as a class of the digital information concerned and creation data, is inserted in 1997, 2-24 (No.683), and a pp.99-124 reference format, and digital information is distributed among a user in these formats. Furthermore, the program of the

intermediate-language format for interpreting and performing embedded digital-watermarking information is prepared.
[0008] Moreover, the server among which the server which enciphers and distributes digital information, such as an image and voice, in order to attain the above-mentioned purpose in this invention, and the user terminal which decodes the this enciphered digital information and performs various processings distribute digital information in the system which it comes to connect through a network saves an encryption key while enciphering the digital information distributed among a user with a common key encryption system.
[0009] A server enciphers the class of digital information, creation data, an expiration date, etc. with the private key of the public key cryptosystem of a server, and gives a digital signature about the information concerned further, and a third person inserts such information and the digital certificate of a server in said enciphered digital information easily in the form of the digital-watermarking information which cannot be distinguished.
[0010] Next, while preparing the program for interpreting and performing digital-watermarking information which was described in the intermediate-language format independent of equipment, and was inserted, the digital information distributed to a user is created by adding the download program for downloading the program concerned from a server to the digital information where digital-watermarking information was embedded.
[0011] It considers as the digital information created by said server when distributing digital information among a user, and when using the digital information as which the user was enciphered, a program is downloaded from a server using the download program added to the distributed digital information.
[0012] A user draws up the digital certificate of the self-signature format containing the public key of a user name and the key pairs concerned etc. while generating the key pair of a public key cryptosystem by performing this downloaded program. The digital-watermarking information inserted in the digital information enciphered by performing the program furthermore downloaded is taken out, and a digital signature is verified about the class of enciphered digital information which took out the public key of a public key cryptosystem about the digital certificate of the server in the taken-out information, and was further taken out from digital-watermarking information, creation data, an expiration date, etc.
[0013] Next, the class of enciphered digital information, creation data, an expiration date, etc. a user's identifier, the digital certificate of a user's self-signature format, and a user's digital signature to such information are transmitted to a server.
[0014] If a server receives the information from a user, receipt information will verify it in the right with the public key picked out from the digital certificate of a user's self-signature format. If a verification result is right, a server will be decoded with the private key of the public key encryption of the server which saves the enciphered information which is included in receipt information, and will verify the class of digital information, creation data, an expiration date, etc. about the received information.
[0015] A digital signature is generated while enciphering with the public key of the user who took out the encryption key which was used in order to encipher digital information, if these verification results are also right, and which is saved, and picked out this encryption key from the digital certificate of a user's self-signature format included in said receipt information. The encryption key information and the digital signature which were enciphered are transmitted to a user.
[0016] If a user receives transmit information, he will verify a digital signature while he decodes the encryption key enciphered with the private key corresponding to the digital certificate of a self-signature format using the downloaded program. The digital information enciphered with the encryption key decoded when the verification result was right is decoded, and the information concerned is processed for a display, printing, etc.
[0017] Moreover, the result in digital cipher processing, such as a decode result of the digital information in a user terminal, all intermediate information, etc. are stored on the storage of the volatility of a user terminal. Furthermore, unjust use of digital contents is prevented by canceling the data concerned on an volatile store immediately by the user terminal, when termination or a

verification result does not have right processing.
[0018] When according to this invention digital information is distributed on a network and a user processes display, playback, etc., the safeguard optimal about the copyright of such digital information can be offered.
[0019]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing.
[0020] Drawing 1 shows an example of the gestalt of operation of the digital information protection system by this invention, the server to which one creates digital contents, the server which distributes among a user the digital contents by which 2 was created by the server 1, and 3 are terminal units (user terminal) which a user uses among drawing, and these are connected in the network which is not illustrated.
[0021] The outline of this system is explained using drawing 1 .
[0022] An implementer creates digital contents by the digital contents creation server 1, and the creation information about the digital contents and these contents which were created etc. is transmitted to the digital contents distribution server 2. About the digital contents which received, the digital contents distribution server 2 creates the digital information for distributing among a user, and distributes it among a user 3 by making these into the encryption contents 4. Distribution to a user may be performed in a network, or you may distribute in the form of a medium like CD-ROM.
[0023] A user 3 transmits the distribution server 2 which transmits predetermined information to the distribution server 2 as a request (use demand) 5 to a user 3 by making into the decode information 6 the encryption key used in order to inspect the contents, and to encipher digital contents if right if a request 5 is received, when using the distributed encryption contents 4. A user 3 returns to the original digital contents using the decode information 6, and performs processing of a display or printing.
[0024] These processings are explained to a detail using drawing 2 thru/or drawing 4 .
[0025] The flow chart which drawing 2 shows the format of the encryption contents 4 in drawing 1 , and shows processing in case drawing 3 creates the digital contents distributed by the digital contents distribution server 2, and drawing 4 are flow charts which show the processing when using the distributed digital contents.
[0026] When creating the information on drawing 2 by the digital contents distribution server 2, the encryption key of the common key encryption system for enciphering digital contents is generated first, and digital information is enciphered using this encryption key (s11). Next, the address of the information about these digital contents, i.e., a class, creation data, an expiration date, an identification number, an implementer, and the digital contents distribution server 2 etc. is enciphered with the public key of the public key cryptosystem of the digital contents distribution server 2 (s12). A digital signature is given to the information created by s12 (s13), and the alteration of the information in the middle of distribution is prevented.
[0027] Next, it embeds in the digital-watermarking format which a third person cannot detect to the encryption digital contents which drew up the digital certificate of the information about the digital contents enciphered by s12, the digital signature created by s13, and the distribution server 2 by s11 (s14).
[0028] Moreover, the executive program which, on the other hand, takes out, interprets and performs information embedded as digital-watermarking information is prepared in the intermediate-language format independent of a model (s15).
[0029] Furthermore, the program for a communication link (download) of the intermediate-language format for downloading the program of s15 is created, and it adds to the information on s14 (s16). The information created by s16 is distributed among a user (s17). As a distribution means, it may carry out electronically using a network, or you may distribute with a gestalt like CD-ROM, and the distribution gestalt is not asked.
[0030] Now, how a user uses the distributed digital information is explained using the flow chart of drawing 4 . Here, s21-s28 are processings of a user terminal 3, and s31-s34 are processings of the distribution server 2.

[0031] A user takes out the intermediate-language program for a communication link for performing download shown in drawing 2 from the distributed digital information (s21). Since this program is the only added [ merely ] format, a user can take out easily. Moreover, since [ like the intermediate-language format independent of a model, for example, a JAVA applet, ], any models can be performed if it has the function to perform an intermediate-language program like JAVA.
[0032] Now, the executive program prepared by s15 of drawing 3 by the download program taken out by s21 is downloaded by the distribution server 2 (s22). Next, while using the executive program downloaded by s22 and generating the key pair of the public key and private key for users in a public key cryptosystem, the digital certificate of the self-signature format of having signed with its own private key is drawn up (s23).
[0033] Next, the information embedded with the gestalt of digital watermarking at the distributed digital information is taken out by the program downloaded by s22 (s24).
[0034] With the public key of the public key cryptosystem of the distribution server 2 contained in the digital certificate in the taken-out information, the digital signature about the class of said enciphered digital contents in the taken-out information, creation data, an expiration date, etc. is verified. If a verification result is right, the private key of a user's public key cryptosystem will perform a digital signature to information, such as a class of enciphered digital contents, creation data, and an expiration date, a user's identifier, and the digital certificate of the self-signature format created by s23 which were taken out by s24 (s25).
[0035] Next, the result which carried out the digital signature to information, such as a class of enciphered digital contents, creation data, and an expiration date, the user name, and the digital certificate of the self-signature format created by s23 which were taken out by s24 is transmitted to the distribution server 2 through a network (s26).
[0036] The digital signature in the information which two is the public key of a user's public key cryptosystem contained in the digital certificate of the self-signature format in the information which it was transmitted and was received, and was this received by the distribution servers26 is verified (s31). If the verification result of a digital signature is right, the encryption information created by processing of drawing 3 of s12 among the information transmitted by the user will be taken out, and it will be decoded with the private key of the public key cryptosystem of the distribution server 2 (s32).
[0037] Verify the class of digital contents, creation data, an expiration date, etc. about the decoded information, and if it is right It takes out from the place which has saved the encryption key used for enciphering the digital contents itself by s11 of drawing 3 (s33). Next, it enciphers with the public key of a user's public key cryptosystem contained in the digital certificate of the self-signature format of the user in the information which received this encryption key, a digital signature is given further, and such information is transmitted to a user 3 through a network (s34).
[0038] A digital signature is verified while decoding the information with the private key of a user's public key cryptosystem, if the information transmitted from the distribution server 2 by processing of a user three s34 is received (s27). If the verification result of a digital signature is right, it decodes using the encryption key which decoded the digital contents enciphered by s11, and the result will be displayed on a screen or will be printed (s28).
[0039] All of these processings in a user terminal 3 are performed and stored on volatile memory, and they are not performed on the storage of a non-volatile. Moreover, the time when a verification result is unjust, and when interrupting processing for the middle, the condition of performing by the user terminal 3, and information are canceled immediately.
[0040]
[Effect of the Invention] As explained above, when according to this invention digital information is distributed on a network and a user processes display, playback, etc., the check of an expiration date etc. is made about such digital information, and unjust use can be prevented.

---

[Translation done.]

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]
[Drawing 1] The system configuration Fig. showing an example of the gestalt of operation of this invention
[Drawing 2] The explanatory view showing the format of the enciphered digital contents distributed among a user
[Drawing 3] The processing flow chart of the creation time of digital contents to distribute
[Drawing 4] The processing flow chart at the time of use of the distributed digital contents
[Description of Notations]
1: A digital contents creation server, a 2:digital contents distribution server, 3:user, 4:encryption contents, 5:request, 6 : decode information.

---

[Translation done.]